# DDoS Detection Model Analysis Report

## Executive Summary

| Metric | Value |
|---|---|
| Dataset Size | 225,711 samples |
| Final Feature Count | 7 |
| Features Removed | 61 |
| Cross-validation AUC | 0.950 (±0.002) |
| Temporal Split AUC | 0.923 |
| Random Split AUC | 0.942 |
| False Positive Rate | 0.3153 |
| False Negative Rate | 0.0011 |

## Top Predictive Features

| Rank | Feature | Importance |
|---|---|---|
| 1 | URG Flag Count | 0.408 |
| 2 | PSH Flag Count | 0.297 |
| 3 | ACK Flag Count | 0.147 |
| 4 | Fwd IAT Min | 0.064 |
| 5 | Idle Std | 0.046 |
| 6 | Bwd IAT Min | 0.038 |
| 7 | FIN Flag Count | 0.000 |

## Recommendations

1. Model shows realistic performance with meaningful trade-offs
2. Consider ensemble methods (Random Forest + XGBoost) for improvement
3. Tune decision threshold to optimize precision/recall balance
4. Test on different DDoS attack types for robustness
5. Consider anomaly detection for unknown attack variants
6. Add domain knowledge features (burst patterns, flow duration bins)
7. Monitor model performance in production environment